ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

May 23, 1997

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARIES OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF

SUBJECT: Implementation of Defense Information Infrastructure Common Operating Environment Compliance

The Defense Information Infrastructure (DII) Common Operating Environment (COE) is a collection of reusable software components, a software infrastructure for supporting mission-area applications, guidelines, standards, and specifications. The DII COE Integration and Runtime Specification (I&RTS), CM-400-01-03, dated 1 January 1997, outlines these guidelines and rules. It describes how to reuse existing software and properly build new software so that integration is seamless, and, to a large extent, automated. The DII COE defines eight progressively deeper levels of integration for the runtime environment. These levels are directly tied to the degree of interoperability achieved. The I&RTS document is the result of the collaboration among the Services, Joint Staff, USD(A&T), ASD(C3I), DISA, DIA and other elements of the Intelligence Community.

All UNIX-based C4I legacy systems, other than mainframe base systems, shall be Level 5 DII COE compliant. All new C4I emerging systems and upgrades shall be level 6 DII COE compliant with the goal of achieving level 7. For those systems not achieving the goal, waivers must be requested using the waiver procedures discussed below (e.g., hardware purchased through competitive procurements may not warrant the investment in porting the entire DII COE to a new computing platform). Level 5 compliance, as defined in the DII COE I&RTS, provides a minimum essential DII compliance that ensures applications are segmented, installable using the COE installation tools, operate with the COE kernel, and can at least federate on a platform. Level 7 provides additional interoperability and economy by using COE services to integrate information, and by requiring that legacy applications do not duplicate the functionality provided by the COE services through the Application Programming Interfaces (APIs).

The Services, Agencies, and other Components are responsible for DII COE compliance (including the enforcement, budgeting, and scheduling). Legacy systems will be migrated based upon costs, schedule, and performance impacts. Waivers may be granted only by the Services, Agencies, or other Component Acquisition Executives based upon the current waiver process specified in the Joint Technical Architecture (JTA).

The DII COE will evolve as necessary to maintain compliance with the JTA. The JTA Version 1.0 stipulates DII compliance as part of its requirements. Version 2.0 of the JTA will mandate the DII compliance levels stipulated above and is expected to be finalized in December, 1997.

Request Director, Joint Staff forward this memorandum to the Unified and Specified Commanders-in-Chief.

My point of contact for this action is Mr. Kevin Meyers who is assigned to the office of my Deputy Assistant Secretary of Defense for Command, Control and Communications, telephone (703) 695-7181.

/s/
Emmett Paige, Jr.